



(19) BUNDESREPUBLIK

DEUTSCHLAND



DEUTSCHES

PATENTAMT

(17) **Patentschrift**  
**(10) DE 196 25 635 C 1**

(51) Int. Cl. 6:

**H 04 L 9/32**

H 04 N 7/16

H 04 N 7/173

- (21) Aktenzeichen: 196 25 635.6-31  
 (22) Anmeldetag: 26. 6. 96  
 (23) Offenlegungstag: —  
 (25) Veröffentlichungstag der Patenterteilung: 4. 12. 97

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

## (73) Patentinhaber:

Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., 80636 München, DE

## (74) Vertreter:

Schoppe, F., Dipl.-Ing.Univ., Pat.-Anw., 81479 München

## (72) Erfinder:

Rump, Niels, Dipl.-Inform., 91054 Erlangen, DE;  
 Zeller, Jürgen, Dipl.-Ing., 91056 Erlangen, DE; Popp,  
 Harald, Dipl.-Ing., 90587 Tuchenbach, DE

## (56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

US	53 69 702
US	53 19 705

## (54) Verschlüsselung und Entschlüsselung von Multimediadaten

(57) Ein Verfahren zum Verschlüsseln von Multimediadaten weist das Eintragen eines Verschlüsselungsindex in einen Bestimmungsdatenblock der Multimediadaten auf, der auf einen zu verwendenden Verschlüsselungsalgorithmus hinweist. Als Reaktion auf den Verschlüsselungsindex in dem Bestimmungsdatenblock wird ein Verschlüsselungsalgorithmus aus einer Mehrzahl von Verschlüsselungsalgorithmen ausgewählt. Unter Verwendung des ausgewählten Verschlüsselungsalgorithmus werden die Multimediadaten verschlüsselt. Verschiedene weitere Einträge in dem Bestimmungsdatenblock, der den Multimediadaten zugeordnet wird, erlauben eine Freischaltung einer Entschlüsselungsvorrichtung, einen schnellen Zugriff auf eine Datenbank von verschlüsselten Multimediadaten sowie eine Kunden- und Daten-spezifische Benutzung der Multimediadaten unter Berücksichtigung urheberrechtlicher Gesichtspunkte.

DE 196 25 635 C 1

DE 196 25 635 C 1

Die vorliegende Erfindung bezieht sich auf die Verschlüsselung und Entschlüsselung von Multimediadaten und insbesondere auf Verschlüsselungs- und Entschlüsselungsformate, die beispielsweise beim kommerziellen Vertrieben von Multimediadaten eingesetzt werden können.

Mit dem Auftreten von Telekommunikationsnetzen und insbesondere aufgrund der großen Verbreitung von Multimediadaten-fähigen Personalcomputern entstand ein Bedarf, digitale Multimediadaten, wie z. B. digitale Audiodaten oder digitale Videodaten, kommerziell zu vertreiben. Die Telekommunikationsnetze können beispielsweise analoge Telefonleitungen, digitale Telefonleitungen, wie z. B. ISDN, oder auch das Internet sein. Unter kommerziellen Anbietern von Multimediaproduktten besteht der Bedarf, Multimediadaten zu verkaufen oder auszuleihen, wobei es einem Kunden möglich seien sollte, aus einem bestimmten Katalog zu jeder Zeit individuell ein bestimmtes Produkt auswählen zu können, das dann selbstverständlich nur von dem Kunden, der dafür bezahlt, benutzt werden kann.

Im Gegensatz zu bekannten verschlüsselten Fernsehprogrammen, wie z. B. den Fernsehkanälen Premiere oder MTV, bei denen die ausgesendeten Daten für alle Benutzer, die gegen eine bestimmte Gebühr eine geeignete Entschlüsselungsvorrichtung erworben haben, gleich verschlüsselt ist, schafft die vorliegende Erfindung Verfahren und Vorrichtungen, die eine individuelle, kundenselektive Verschlüsselung und Entschlüsselung von Multimediadaten ermöglichen. Im Gegensatz zu den genannten Fernsehkanälen, die ein festes Programm vorgeben, für das sich der Benutzer komplett entscheiden muß, ermöglichen die Verfahren und Vorrichtungen der vorliegenden Erfindung eine maximale Wahlfreiheit des Kunden, d. h. derselbe muß nur für die Produkte bezahlen, die er tatsächlich auch benutzt hat.

Das US-Patent Nr. 5,369,702 offenbart ein System zum Erhöhen der Sicherheit eines Computersystems, wobei einzelne Benutzer dasselbe flexibel und effizient nützen können. Das in dieser Schrift offenbarte Verfahren umfaßt die Schritte des Zugreifens auf einen objektorientierten Schlüsselverwalter, des Auswählens eines zu verschlüsselnden Objekts, des Auswählens einer Etikette für das Objekt, des Auswählens eines Verschlüsselungsalgorithmus, des Verschlüsselns des Objekts gemäß dem Verschlüsselungsalgorithmus, des Etikettierens des verschlüsselten Objekts, des Lesens des Objektetikets, des Bestimmens einer Zugriffsermächtigung basierend auf dem Objektetikett und des Entschlüsselns des Objekts, wenn die Zugriffsermächtigung erteilt ist. Eine Datei- "Etikette" besteht aus einer Serie von Buchstaben oder Zahlen, welche verschlüsselt oder nicht verschlüsselt sein können.

Das US-Patent Nr. 5,319,705 betrifft ein Verfahren und ein System zum sicheren Verteilen einer Mehrzahl von Softwaredateien von einem Softwareverteilsprozessor zu einem Benutzerprozessor, während der Benutzerprozessor selektiv in die Lage versetzt wird, nur eine Teilmenge einer kleineren Mehrzahl von Softwaredateien zu verwenden. Dies wird durch Verwenden eines Kundenschlüssels erreicht, welcher einen unverschlüsselten Kundenschlüssel und einen abgeleiteten Abschnitt aufweist, der aus der Kundennummer abgeleitet ist.

Die Aufgabe der vorliegenden Erfindung besteht darin, Verfahren und Vorrichtungen zum Verschlüsseln und

Entschlüsseln von Multimediadaten zu schaffen, welche zum einen einen wirksamen Urheberrechtsschutz garantieren, und welche zum anderen in der Lage sind, individuell angeforderte Daten flexibel zu ver- bzw. entschlüsseln.

Diese Aufgabe wird durch ein Verfahren gemäß Anspruch 1, durch ein Verfahren gemäß Anspruch 19, durch eine Vorrichtung gemäß Anspruch 25 und durch eine Vorrichtung gemäß Anspruch 27 gelöst.

- 10 Der Erfindung liegt die Erkenntnis zugrunde, daß ein ausreichender Urheberrechtsschutz für Audio- und Videoprodukte, welche in Form von digitalen Multimediadaten vorliegen, nur dann gewährleistet werden kann, wenn möglichst unmittelbar nach der Produktion der digitalen Multimediadaten, die beispielsweise gemäß dem bekannten Standard MPEG Audio Layer 3 codiert bzw. komprimiert sind, eine sichere Verschlüsselung durchgeführt wird. Für Fachleute ist es offensichtlich, daß die vorliegende Erfindung nicht auf die Verwendung von Daten in dem Format MPEG Layer 3 begrenzt ist, sondern daß auch unkomprimierte Multimediadaten oder nach irgendeinem anderen Verfahren komprimierte Multimediadaten ebenfalls verwendet werden können.

Nachdem die Multimediadaten vor ihrer Speicherung/Lagerung von einer Verschlüsselungsvorrichtung verschlüsselt worden sind, können sie individuell von einem Benutzer angefordert werden, der sich im Besitz einer geeigneten Entschlüsselungsvorrichtung befindet. Diese Entschlüsselungsvorrichtung darf jedoch nur zur Durchführung ihrer Aufgaben den Verschlüsselungsschutz um die Daten herum lösen, wobei ebenfalls von großer Bedeutung ist, daß nicht jede Entschlüsselungsvorrichtung in der Lage ist, die Multimediadaten zu lesen, sondern nur die Entschlüsselungsvorrichtung, die sich bei dem Kunden befindet, der für die Multimediadaten bezahlt hat. Ferner ist es wichtig, daß es dem Benutzer möglichst schwer wenn nicht unmöglich gemacht wird, die Multimediadaten selbst sowie die Verschlüsselung unerlaubt zu verändern.

Sollte ein Benutzer versuchen, die Multimediadaten zu verändern, dann ist es wünschenswert, daß die Daten vollständig unlesbar sind. Die Tatsache, daß die Verschlüsselungsvorrichtung bereits an ihrem Ausgang verschlüsselte Dateien erzeugt, den Schutz gewissermaßen sofort über die Multimediadaten legt, gewährleistet also, daß keine ungeschützten Daten am Beginn einer Übertragungs/Speicherungs-Kette auftreten.

Die Entschlüsselungsvorrichtung ist in der Lage, die speziell verschlüsselten Daten zu lesen. Das Verfahren zum Verschlüsseln von Multimediadaten gemäß der vorliegenden Erfindung erzeugt zusätzlich zu vorliegenden unverschlüsselten Multimediadaten einen Bestimmungsdatenblock, in dem sich verschiedene Informationen bezüglich der Verschlüsselung der unverschlüsselten Multimediadaten sowie bezüglich allgemeiner und spezieller Funktionen, die von der vorliegenden Erfindung ausgeführt werden können, befinden.

Einige der Funktionalitäten, die von einer Entschlüsselungsvorrichtung gemäß der vorliegenden Erfindung gefordert werden, werden nachfolgend beschrieben:

Eine Entschlüsselungsvorrichtung der vorliegenden Erfindung soll in der Lage sein, einen Demoabspieler für Audiodaten in dem Format ISO MPEG Layer 3 zu implementieren, welcher es nur zuläßt, daß etwa die ersten 20 Sekunden einer Audioaufzeichnung abgespielt werden. Unter bestimmten Umständen soll es nun möglich sein, daß der Demoabspieler bei einem bestimmten

Kunden bestimmte Musikstücke läuft als 20 Sekunden abspielt. Dies wird durch eine sogenannte Freischaltung des Bitstroms erreicht, welche durch bestimmte in dem Bestimmungsdatenblock vorhandene Einträge bewirkt wird.

Weiterhin soll die vorliegende Erfindung in der Lage sein, eine Entschlüsselungsvorrichtung, d. h. einen Abspieler, für Audiodaten im Format MPEG Layer 3 zu implementieren, der es nur bestimmten Kunden erlaubt, eine bestimmte Audiodatei abzuspielen. Dies dient zum Urheberrechtsschutz für Audio- bzw. Videowerke, wobei ein Abspielen lediglich nach Bezahlung einer Gebühr möglich sein soll.

Zusätzlich soll die vorliegende Erfindung einen Spieler implementieren, der nicht nur den Inhalt einer Audiodatendatei abspielen kann, sondern der auch bestimmte Zusatzinformationen anzeigen kann. Diese Zusatzinformationen (d. h. Metadaten) können Informationen über den Künstler, die Abspielzeit, und weitere Informationen über die Audioaufzeichnung oder beispielsweise auch ein Bild der Schallplatten- oder der CD-Hülle sein.

Eine Verschlüsselungsvorrichtung gemäß der vorliegenden Erfindung ist in der Lage, Multimediadaten effizient und sicher zu verschlüsseln. Ferner implementiert die vorliegende Erfindung eine spezielle Funktionalität, welche Herausforderungs-Antwort-Verfahren genannt wird und später detailliert beschrieben ist.

Dieses Verfahren erlaubt das Erzeugen von vorverschlüsselten Audiodaten, die in einer Datenbank gespeichert sind, auf die ein Kunde sehr schnell zugreifen kann, welcher einen privaten Schlüssel verwendet, der von dem tatsächlich verwendeten Schlüssel zur Verschlüsselung der Daten abgeleitet ist, wobei sich der Kunde unter Verwendung seines privaten Schlüssels und seines Benutzerindexes den tatsächlich verwendeten Schlüssel zur Verschlüsselung selbst berechnen kann, wonach die abgerufenen Multimediadaten entschlüsselt werden können, um sie beispielsweise abzuspielen.

Damit ist es möglich, daß für viele Kunden, die das gleiche Stück abrufen, das Stück nicht jedesmal vollständig für jeden einzelnen Kunden verschlüsselt werden muß, sondern daß die Daten für alle Kunden gleich verschlüsselt werden können, wobei jedoch jeder Kunde den tatsächlich verwendeten Schlüssel unter Verwendung seines Privatschlüssels und eines von der Verschlüsselungsvorrichtung mitgeteilten Antwortschlüssels selbst berechnen kann.

Bei dem Herausforderungs-Antwort-Verfahren wird die individuelle Verschlüsselung für jeden einzelnen Benutzer also nicht durch eine vollständige Neuverschlüsselung der Multimediadaten erreicht, sondern nur durch eine vergleichsweise geringe Änderung in dem Bestimmungsdatenblock, der gemäß der vorliegenden Erfindung zu den Multimediadaten hinzugefügt wird.

Die Verschlüsselung gemäß der vorliegenden Erfindung erzeugt also ein Dateiformat zum Schutz von Multimediadaten, welches bei der Entschlüsselung gemäß der vorliegenden Erfindung verwendet wird, um beispielsweise die oben beschriebenen Funktionalitäten zu implementieren.

Ein bevorzugtes Ausführungsbeispiel der vorliegenden Erfindung wird nachfolgend bezugnehmend auf die beiliegenden Zeichnungen detaillierter erläutert. Es zeigen:

Fig. 1 einen festen Teil eines Bestimmungsdatenblocks;

Fig. 2 einen variablen Teil eines Bestimmungsdatenblocks;

Fig. 3 eine Aufteilung von Multimediadaten in verschlüsselte Daten und unverschlüsselte Daten;

Fig. 4 einen Hüllenblock für die verschiedenen Einträge im variablen Teil des Bestimmungsdatenblocks;

Fig. 5 eine Übersicht von für einzelne Funktionalitäten benötigten Einträgen in den Bestimmungsdatenblock.

Jede Multimediaschutz-Datei (MMP-Datei; MMP = Multi Media Protection), welche im Nachfolgenden auch als MMP-Datenstrom bezeichnet wird, wird von einem speziellen MMP-Bestimmungsdatenblock begleitet. Nachfolgend wird das Format dieses Bestimmungsdatenblockes erörtert.

Der Bestimmungsdatenblock besteht aus zwei Teilen, und zwar aus einem festen Teil 10, welcher in Fig. 1 gezeigt ist, und aus einem variablen Teil 30, der in Fig. 2 gezeigt ist. Der feste Teil 10 des Bestimmungsdatenblocks, der aus 10 und 30 besteht, enthält allgemein gesagt Minimalinformationen, wie z. B. Informationen, wie der Bestimmungsdatenblock verschlüsselt ist, wie lange derselbe ist und wo ein potentiell vorhandener nächster Bestimmungsdatenblock zu finden ist. Die Einträge in den festen Teil des Bestimmungsdatenblocks (10, 30) werden nachfolgend einzeln beschrieben.

In der in Fig. 1 gezeigten Tabelle bezeichnet die erste Spalte den Namen des jeweiligen Eintrags, die zweite Spalte die Größe desselben, die dritte Spalte den(die) Name(n) von möglichen Untereinträgen, die vierte Spalte die jeweilige Größe des einzelnen Untereintrags, während die letzte Spalte der Tabelle in Fig. 1 anzeigt, ob der Eintrag, d. h. die derselben zugeordneten Untereinträge, verschlüsselt sind oder nicht.

Die erste Zeile 12 enthält einen Dateiindex, der als Untereintrag einen Identifizierer bezüglich einer speziellen MMP-Datei sowie eine Versionsnummer derselben aufweist. In Zeile 14 befindet sich ein Längenindex, welcher die Länge des Bestimmungsdatenblocks anzeigt. Dieser Eintrag dient beispielsweise zum Überspringen des Bestimmungsdatenblocks oder auch zum einfacheren Parsen. In Zeile 16 bezeichnet ein Versatzindex den Versatz von einem Bestimmungsdatenblock zu einem nächsten Bestimmungsdatenblock, wobei derselbe nützlich ist, um z. B. im Falle von mehreren Bestimmungsdatenblöcken in einer einzigen MMP-Datei von einem Bestimmungsdatenblock zum nächsten Bestimmungsdatenblock springen zu können, ohne immer den Dateiindex auf Übereinstimmung prüfen zu müssen.

Eine Zeile 18 der Tabelle in Fig. 1 enthält einen Verschlüsselungsindeks, welcher ein Index für eine Tabelle von Verschlüsselungs- und Entschlüsselungsalgorithmen ist, welche verwendet werden, um entscheidende Teile des Bestimmungsdatenblocks für nicht autorisierte Benutzer oder Programme unlesbar zu machen. Bei einer Implementierung der vorliegenden Erfindung können 65 535 verschiedene Verschlüsselungsalgorithmen verwendet werden, welche in einer Urheberrechtsbibliothek abgelegt sind, die sowohl in der Verschlüsselungsvorrichtung als auch in der Entschlüsselungsvorrichtung gemäß der vorliegenden Erfindung vorhanden sein muß. Auf einen dieser 65 535 verschiedenen Verschlüsselungsalgorithmen wird über die ersten zwei Byte (d. h. den ersten Untereintrag Verfahren) zugegriffen. Der zweite Untereintrag Schlüssel liefert einen Index für eine Tabelle, in der ein Satz von Verschlüsselungsschlüsseln oder Schlüsseln für jeden Ver-

schlüsselungsalgorithmus gesperrt sein kann. Diese Tabelle von Schlüsseln für jeden einzelnen Verschlüsselungsalgorithmus muß ebenfalls sowohl in der Verschlüsselungsvorrichtung als auch in der Entschlüsselungsvorrichtung der vorliegenden Erfindung vorhanden sein.

Bei der vorliegenden Erfindung wird also zum Verbzw. Entschlüsseln ein sogenanntes symmetrisches Verschlüsselungsverfahren verwendet, was bedeutet, daß sowohl die Verschlüsselungsvorrichtung als auch die Entschlüsselungsvorrichtung im Besitz sowohl der Verschlüsselungsverfahren als auch besonders der Schlüssel selbst sein müssen. Zur Ausführung der Erfindung würde es jedoch auch genügen, lediglich den Verschlüsselungsalgorithmus in dem Verschlüsselungsindex 18 zu bestimmen. In diesem Fall könnte der Schlüssel selbst beispielsweise vorgegeben sein. Dieses Ausführungsbeispiel würde jedoch einen geringeren Schutz als das vorher beschriebene Ausführungsbeispiel mit Algorithmus und Schlüssel liefern.

Hinter dem Eintrag 18 in dem Bestimmungsdatenblock befindet sich der variable Teil 30 des Bestimmungsdatenblocks, der in Fig. 2 gezeigt ist und später beschrieben wird. Hinter dem variablen Teil des Bestimmungsdatenblocks befindet sich noch ein letzter Eintrag 20, der Prüfsumme genannt wird. Diese Prüfsumme besteht aus einem sogenannten MD5-Fingerabdruck, der detaillierter in der RFC1321 beschrieben ist. Zum Verständnis der vorliegenden Erfindung soll er jedoch kurz ausgeführt werden. MD5 ist ein Algorithmus, der eine beliebige Anzahl von Datenbyte in eine Zahl mit einer Länge von 128 Bit (= 16 Byte) abbildet. Die MD5-Abbildung (MD5 = Message Digest 5) hat die Eigenschaft, daß auch die geringste Änderung in den Eingangsdaten eine völlig andere MD5-Zahl erzeugt. Daher wird MD5 benutzt, um aus Daten beliebiger Länge einen Fingerabdruck fester Größe zu erzeugen. In dem Eintrag 20 Prüfsumme befindet sich bei einem Ausführungsbeispiel der vorliegenden Erfindung beispielsweise ein MD5-Fingerabdruck des Bestimmungsdatenblocks (10, 30). Ein anderes Ausführungsbeispiels könnte im Eintrag Prüfsumme 20 beispielsweise sowohl den Bestimmungsdatenblock als auch eine vorbestimmte Anzahl von zu verschlüsselnden Multimediataten aufweisen, denen der beschriebene Bestimmungsdatenblock zugeordnet ist. Dadurch definiert der Eintrag 20 eindeutig und manipulatorsicher (der Eintrag 20 ist zusätzlich noch verschlüsselt) die Zuordnung eines Bestimmungsdatenblocks zu den Multimediataten.

Alle Einträge in den Bestimmungsdatenblock, d. h. auch die Einträge des nachfolgend beschriebenen variablen Teils des Bestimmungsdatenblocks, sind in der so genannten "Big Endian"-Bytereihenfolge. Als "Big Endian" wird eine Übertragung/Speicherung bezeichnet, bei der das höchstwertige Byte als erstes übertragen/gespeichert wird. Ein Beispiel soll dies veranschaulichen. Ein Datum ist beispielsweise vier Byte groß, d. h. sein Wert lautet  $0 \times 56fe4321$ . Nach der "Big Endian"-Bytereihenfolge wird  $0 \times 56$  zuerst übertragen/gespeichert, woraufhin  $0 \times fe$ ,  $0 \times 43$  und  $0 \times 21$  folgen.

Wie bereits angemerkt wurde, ist in Fig. 2 eine tabellarische Darstellung des variablen Teils 30 des Bestimmungsdatenblocks gezeigt. Die erste Spalte der Tabelle in Fig. 2 bezeichnet eine Identifikationsnummer (ID) der einzelnen Einträge. Die zweite Spalte enthält den Namen des Eintrags, dessen Größe in der dritten Spalte angegeben ist. Die vierte Spalte zeigt wiederum analog zu der Tabelle in Fig. 1 den Namen des einzelnen Unter-

reintrags oder potentiell mehrerer Untereinträge, deren Größe wiederum in der vorletzten Spalte angegeben ist. Die letzte Spalte zeigt genauso wie in Fig. 1 an, ob der einzelne Eintrag verschlüsselt ist oder nicht.

Der variable Teil 30 des Bestimmungsdatenblocks enthält unter anderem Informationen bezüglich der urheberrechtlichen Verschlüsselung des Audiobitstroms, d. h. der Multimediataten. Nachfolgend werden die Einträge in den variablen Teil des Bestimmungsdatenblocks und ihre Funktionen bzw. Aufgaben im einzelnen beschrieben.

In Spalte 32 befindet sich ein Mengenindex, welcher aus zwei Untereinträgen d. h. Schritt und Menge besteht. Der erste Untereintrag Schritt gibt, wie es in Fig. 3 detaillierter dargestellt ist, die Gesamtmenge von Multimediataten an, die dem speziellen Bestimmungsdatenblock zugeordnet sind. Um Multimediataten auf einfache Weise speichern oder übertragen zu können, empfiehlt es sich, die Multimediataten, d. h. den Bitsstrom, in einzelne Datenblöcke mit überschaubarer Länge zu unterteilen, denen dann ein Bestimmungsdatenblock zugeordnet wird. Dies bedeutet, daß z. B. ein Musikstück mehrere Bestimmungsdatenblöcke aufweist, welche möglicherweise für ein einzelnes Musikstück mehrere verwendete Verschlüsselungsalgorithmen bezeichnen können.

Aufgrund der Tatsache, daß bei einem Ausführungsbeispiel der vorliegenden Erfindung die Audiodaten im MPEG Layer 3 Format vorliegen, welches bereits eine hohe Kompression der Audiodaten bewirkt, ist es im Sinne einer effizienten, zeitsparenden Ausführung der vorliegenden Erfindung ausreichend, lediglich einen bestimmten Teil eines Bestimmungsdatenblocks zugewiesenen Datenblocks zu verschlüsseln und nicht den gesamten Datenblock zu verschlüsseln. Dies kann gemacht werden, da bei der Verwendung von hochkomprimierten Multimediaformaten schon ein sehr kleiner Teil von Störungen, d. h. Verschlüsselungen, gravierende Auswirkungen hat, da die hochkomprimierten Daten bereits eine minimale Informationsredundanz besitzen. Dieser Anteil der verschlüsselten Daten ist durch den Untereintrag Menge in dem Mengenindex 32 bezeichnet. Fig. 3 stellt also die Aufteilung eines Datenblocks in die verschlüsselten Daten und in die aus Wirtschaftlichkeitsgründen unverschlüsselt gelassenen Daten dar. Der Untereintrag Schritt muß durch den Eintrag Menge teilbar sein, um ein korrektes Ver- bzw. Entschlüsseln sicherzustellen. Für Fachleute ist es jedoch offensichtlich, daß die vorliegende Erfindung ebenso auch eine Vollverschlüsselung vornehmen kann, bei der Schritt gleich Menge ist, während bei einer Teilverschlüsselung Schritt größer als Menge ist.

Eine Zeile 34 in Tabelle 2 bezeichnet einen Lieferantenindex, wobei der Lieferantenindex einen numerischen Wert aufweist, der auf den Inhaber der Urheberrechte der in dem Datenblock verschlüsselten Multimediataten hinweist, der für eine Verwendung der Multimediataten in dem Datenblock bezahlt werden muß.

In einem Eintrag 36 mit der Bezeichnung Großhändlerindex befindet sich ein numerischer Wert, der den Großhändler der in dem Datenblock vorhandenen Multimediataten bezeichnet.

In Zeile 38 der Tabelle in Fig. 2 befindet sich ein Benutzerindex, welcher auf den Kunden/Benutzer hinweist, an den die in dem Datenblock vorhandenen Multimediataten übermittelt, z. B. verkauft oder ausgeliehen wurden.

Ein Flagindex 40 enthält drei verschiedene Flags, die

als Geheim, als Registrierung und Herausforderung bezeichnet sind. Die Flag Geheim zeigt an, daß bei der Verschlüsselung der Großhändlerindex verwendet werden soll. Wenn diese Flag gesetzt ist, wird das Verschlüsselungs/Entschlüsselungs-Verfahren den Großhändlerindex als einen Eintrag in eine Direktzugriffstabelle benützen, um den für einen bestimmten Verschlüsselungs/Entschlüsselungs-Algorithmus erforderlichen Schlüssel zu erhalten. Dieser Eintrag ermöglicht eine Großhändler-spezifische Identifizierung von Multimediadaten, d. h. ein Benutzer/Kunde wird z. B. in der Lage sein, alle Produkte von einem spezifischen Großhändler zu beziehen.

Die Flag Registrierung zeigt an, daß sowohl der Lieferantenindex als auch der Benutzerindex bei der Verschlüsselung verwendet werden sollen. Das Verschlüsselungs/Entschlüsselungs-Verfahren wird dieses Paar (Großhändlerindex, Benutzerindex) beim Adressieren einer Direktzugriffstabelle verwenden, wodurch der Schlüssel für einen speziellen Verschlüsselungsalgorithmus erhalten werden kann. Diese Flag ermöglicht zusammen mit den jeweiligen Einträgen, daß ein Großhändler einzelne Benutzer spezifisch bedienen kann.

Die Herausforderungsflag zeigt an, daß der Kunde einen Herausforderungsindex 44 und seinen Benutzerindex verwendet hat, um eine MMP-Datei zu erhalten, wobei der Herausforderungsindex 44 und ein Antwortindexeintrag 46 in dem variablen Teil des Bestimmungsdatenblocks verschlüsselt sind. Eine detailliertere Beschreibung des Herausforderungs-Antwort-Verfahrens gemäß der vorliegenden Erfindung wird später durchgeführt. Selbst wenn nicht alle 32 möglichen Flags verwendet werden, muß bei einem Ausführungsbeispiel der vorliegenden Erfindung die Gesamtlänge von 4 Byte geschrieben, gesendet und gelesen werden. Alle unbunutzten Bits werden ignoriert, dieselben müssen jedoch auf Null gesetzt sein. Es ist ebenfalls möglich, alle drei Flags zu senden. In diesem Fall werden alle 3 Schlüssel verwendet, und zwar einer nach dem anderen.

Eine Zeile 42 der Tabelle von Fig. 2 enthält einen Freiindex. Dieser Freiindex 42 enthält zwei Untereinträge, d. h. Seriennummer und Benutzerdaten. Der Untereintrag Seriennummer enthält eine 32-Bit-lange Seriennummer, die die Multimediadaten identifiziert. Der Untereintrag Benutzerdaten, d. h. die nächsten 96 Bits des Eintrags Freiindex 42, sind mit den ersten 12 Byte des MD5-Fingerabdrucks der ersten Daten des Multimediadatenblocks von Menge bis Schritt minus Menge gefüllt.

Der gesamte Eintrag Freiindex 42 im variablen Teil des MMP-Bestimmungsdatenblocks ist verschlüsselt, wie es in der letzten Spalte in Fig. 2 gezeigt ist. Ferner ist die Prüfsumme 20 des Bestimmungsdatenblocks selbst verschlüsselt, d. h. kein Unberechtigter wird in der Lage sein, eine MMP-Bestimmungsdatenblock mit einem bestimmten MD5-Fingerabdruck zu erzeugen. Der Freiindex 42 liefert damit eine eindeutige Zuordnung des Bestimmungsdatenblocks (10, 30) zu den verschlüsselten oder auch unverschlüsselten Multimediadaten. Bei einer Wiedergabe d. h. einer Entschlüsselung wird nun überprüft, ob die aus den Multimediadaten errechnete MD5-Zahl mit der MD5-Zahl, die im Untereintrag Benutzerdaten vorhanden ist, übereinstimmt. Da bei jeder Änderung der Multimediadaten mit sehr hoher Wahrscheinlichkeit die MD5-Zahl derselben verschieden sein wird, ist anzunehmen, daß die zu schützenden Daten nicht verändert wurden, wenn die beiden MD5-Zahlen übereinstimmen.

Der Freiindex 42 wird für das bereits anfangs erwähnte Freischaltungsverfahren verwendet, welches ein Demospeler (eine Demoentschlüsselungsvorrichtung) implementieren kann. Die Untereinträge Seriennummer 5 und Benutzerdaten in dem Freiindex 42 werden unter Verwendung der Bool'schen-Verknüpfung XOR kombiniert und mit einem Wert verglichen, der von dem Demospeler verwendet wird, d. h. auf den der Demospeler eingestellt bzw. eingerichtet ist. Wenn dieser Wert 10 mit der Kombination von Seriennummer und Benutzerdaten übereinstimmt, wird die MMP-Datei freigeschaltet und kann länger als etwa 20 Sekunden gespielt werden. Falls diese Übereinstimmung nicht vorhanden ist, wird der Demospeler nicht freigeschaltet, weshalb der 15 selbe das Abspielen, d. h. das Entschlüsseln, der Multimediadaten in der MMP-Datei abbricht. Die Freischaltung selbst dient also dazu, ein zur Wiedergabe benutztes Produkt, d. h. die Entschlüsselungsvorrichtung, zu modifizieren. Eine Entschlüsselungsvorrichtung, welche 20 die vorliegende Erfindung ausführen kann, kann beispielsweise Win Play 3 sein. Die Entschlüsselungsvorrichtung kann beispielsweise kostenlos als eine Demo-version bei allen Benutzern erhältlich sein. Sie wird jedoch auf eine Weitergabe von Multimediadaten mit einer Länge von beispielsweise 20 Sekunden beschränkt 25 sein. Sobald allerdings ein MMP-Bitstrom mit gültigem Freiindex 42 erkannt wird, wird die Entschlüsselungsvorrichtung freigeschaltet. Dieselbe stellt also für die Wiedergabe einer MMP-Datei mit gültigem Freiindex 30 42 eine Vollversion ohne Begrenzung dar. Die Freischaltung mittels des Freiindex 42 hat also nichts mit der Bezahlung der geschützten Multimediadaten zu tun, sondern lediglich mit der Nutzung einer Demoversion der Entschlüsselungsvorrichtung. Aus technischen und politischen Gründen ist es nämlich oft einfacher, daß nicht die Entschlüsselungsvorrichtung selbst insgesamt bezahlt wird, sondern daß pro Multimediatei eine kleine Summe für die Nutzung der Entschlüsselungsvorrichtung vom Großhändler oder Lieferanten, der den 35 Freiindex 42 codiert hat, abgeführt wird.

In Zeile 44 und Zeile 46 der Tabelle in Fig. 2 befinden sich der Herausforderungsindex bzw. der Antwortindex. Der Herausforderungsindex 44 weist als Untereinträge den Codierertyp (Entschlüsselungsvorrichtungstyp), die Codiererversion, den Codiererzustand, den Großhändlerindex, den Benutzerindex und Benutzerdaten auf. Sowohl der Herausforderungsindex 44 als auch der Antwortindex 46 sind verschlüsselt.

Das Herausforderungs-Antwort-Verfahren kann verwendet werden, um eine große Datenbank von MMP-Dateien zu erzeugen, welche Multimediadaten enthalten. Die MMP-Datenbank besteht aus MMP-Dateien, die mit einem in dem Untereintrag Schlüssel in dem Verschlüsselungsindex 18 bezeichneten Schlüssel k verschlüsselt sind. Ein Kunde wird auf diese Datenbank zugreifen, indem er zwei Hilfsschlüssel zu derselben sendet. Diese beiden Hilfsschlüssel sind der Benutzerindex u 38 und ein Benutzer-definierter Privatschlüssel p, der auch als der Herausforderungsindex 44 bezeichnet wird. Der Hilfsschlüssel u sowie der Hilfsschlüssel p sind also bei einem Kunden, d. h. bei einer speziellen Entschlüsselungsvorrichtung, vorhanden. Der Kunde sendet nun die beiden Hilfsschlüssel u und p zu einer Datenbank, die eine Vielzahl von MMP-Dateien enthält, um bestimmte Multimediadaten von derselben abzurufen. Die Datenbank, die die Multimediateien enthält, sendet nun eine MMP-Datei zu dem Kunden zurück, welche den Antwortindex r 46 enthält. Dieser Antwortin-

dex r wird aus der EXKLUSIV-ODER-Verknüpfung des Schlüssels k, des Benutzerindex u und des Herausforderungsindex p berechnet. Die Entschlüsselungsvorrichtung des Kunden empfängt nun die MMP-Datei von der Verschlüsselungsvorrichtung, die die MMP-Datenbank halten kann, wobei diese Datei nun den gerade berechneten Antwortindex 46 enthält. Die Entschlüsselungsvorrichtung ist nun in der Lage, den zur Entschlüsselung der Multimediataten notwendigen Schlüssel k aus der EXKLUSIV-ODER-Verknüpfung des Antwortindex r, des Benutzerindex u und des Herausforderungsindex p ihrerseits zu berechnen. Somit liegt in der Entschlüsselungsvorrichtung des Kunden/Benutzers der Schlüssel k vor, wodurch dieselbe die dem Bestimmungsdatenblock zugeordneten Multimediataten entschlüsseln kann.

Der Hintergrund zur Implementierung des Herausforderung-Antwort-Verfahrens liegt in einer effizienten und zeitsparenden Verschlüsselung bzw. Entschlüsselung. Eine Verschlüsselungsvorrichtung hat mit einem Schlüssel k (Verschlüsselungsindex 18, Untereintrag Schlüssel) und mit einem Algorithmus a (Verschlüsselungsindex 18, Untereintrag Verfahren) Multimediataten geschützt. Diese werden zusammen mit k und a in eine MMP-Datenbank eingespeist. Möchten nun beispielsweise 1000 Kunden diese Multimediataten beziehen, müßte ohne das Herausforderungs-Antwort-Verfahren die geschützte Kopie der Multimediataten 1000mal entschlüsselt und für einen speziellen Kunden wieder verschlüsselt werden. Durch das Herausforderungs-Antwort-Verfahren wird nun ein von einer speziellen Entschlüsselungsvorrichtung abhängiger Herausforderungsindex 44 zusammen mit dem daraus resultierenden Antwortindex 46 in den MMP-Datenbestimmungsblock eingetragen. Der gesamte Datenstrom der Multimediataten muß also nicht für jeden Kunden einzeln geändert werden. Es ist also einfacher, beispielsweise 1000mal aus einem Herausforderungsindex 44 einen Antwortindex 46 zu erzeugen und diesen in den Bestimmungsdatenblock einzutragen, als 1000mal die gesamte MMP-Datei zu entschlüsseln und wieder kundenspezifisch zu verschlüsseln.

Eine Zeile 48 des variablen Teils des Bestimmungsdatenblocks enthält einen Auslaufindex, der das Datum kennzeichnet, zu dem die Lizenz des Benutzers, Multimediataten zu verwenden, auslaufen wird. Derselbe ist z. B. in Sekunden gegeben, die seit Mitternacht des 1. Januar 1970 vergangen sind. Es wird darauf hingewiesen, daß der Bereich des Auslaufindex etwa bis zum Jahr 2106 ausreichend sein wird. Selbst wenn dieser Eintrag nicht verschlüsselt ist, wird es schwierig sein, denselben zu ändern, da der Auslaufindex ebenfalls die Prüfsumme 20 (den MD5-Fingerabdruck) des Bestimmungsdatenblocks verändern wird, welche zusätzlich noch verschlüsselt ist.

Eine Zeile 50 enthält einen Multimediaindex, welcher bei einem bevorzugten Ausführungsbeispiel ein ISRC-Code (ISRC = International Standard Record Code) sein kann. Dieser Multimediaindex identifiziert jedes einzelne Musikstück nach international anerkannter Norm. Der ISRC-Code identifiziert ebenfalls den Inhaber d. h. den Lieferanten im Sinne dieser Anmeldung, des Musikstücks, der die Urheberrechte besitzt.

In einer Zeile 52 ist schließlich ein Benutzercodeindex vorgesehen, welcher verwendet wird, um ein Musikstück zu identifizieren, welches keinen ISRC-Code, d. h. keinen allgemein gültigen Multimediaindex, besitzt.

Für Fachleute ist es offensichtlich, daß der Bestim-

mungsdatenblock insbesondere der variable Teil des Bestimmungsdatenblocks, beliebig erweitert werden kann, um beispielsweise weitere Metainformationen, wie z. B. Informationen über den Interpreten oder

5 Künstler von Multimediataten, zusammen mit der Multimediatei zu übertragen und gegebenenfalls zu verschlüsseln. Bei einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung geht jedem Eintrag 32 bis 52 in dem variablen Teil 30 des Bestimmungsdaten-

10 blocks ein Hüllenblock 54 voraus, der in Fig. 4 gezeigt ist. Dieser Hüllenblock liefert Informationen, welcher Eintrag in den variablen Teil 30 des Bestimmungsdatenblocks demselben folgt (Eintragidentifikation), sowie Informationen über die Länge dieses speziellen Eintrags

15 (Eintraglänge). Die Größe des Hüllendatenblocks 54 beträgt jeweils 4 Byte. Dies ist der Grund, daß die Bit-Zahl in der vorletzten Spalte der in Fig. 2 gezeigten Tabelle immer vier Byte kleiner als die in der dritten Spalte gezeigte Bytezahl ist.

20 Wie bereits angemerkt wurde, zeigen die letzte Spalte der Tabelle 1 sowie der Tabelle 2 an, ob der entsprechende Eintrag verschlüsselt ist. Die einzigen verschlüsselten Einträge in den variablen Teil des Bestimmungsdatenblocks, die verschlüsselt sind, sind der Freiindex 42,

25 der Herausforderungsindex 44 und der Antwortindex 46. Alle nicht verschlüsselten Einträge sind jedoch zusätzlich durch den Eintrag Prüfsumme 20 in den festen Teil 10 des Bestimmungsdatenblocks geschützt, da die Prüfsumme zum einen verschlüsselt ist und zum anderen durch den MD5-Algorithmus bereits eine kleine Änderung der Eingabe zu einer wesentlichen Änderung des Ergebnisses desselben führen wird.

29 Für Fachleute ist es offensichtlich, daß z. B. auch fast alle Einträge oder mehr oder weniger als bei dem be-

35 schriebenen bevorzugten Ausführungsbeispiel ver-

30 schlüsseln sein können. Eine Begrenzung der zu ver- schlüsselnden Daten auf die für einen ausreichenden Schutz notwendige Anzahl führt jedoch zu einer wirt- schaftlichen Ausführung der vorliegenden Erfindung,

35 wie es auch im Zusammenhang mit dem Eintrag Mengenindex 32 beschrieben wurde, da es nicht notwendig ist, die gesamten Multimediataten oder den gesamten Bestimmungsdatenblock, sondern lediglich einen Teil

40 derselben zu verschlüsseln, um das unberechtigte Lesen der gesamten Daten unmöglich zu machen. Ferner ist es für Fachleute offensichtlich, daß es sinnlos ist, den Ver-

45 schlüsselungsindex 18 selbst zu verschlüsseln, da die Entschlüsselungsvorrichtung zuerst diesen Eintrag lesen muß, um den Algorithmus und potentiell den Schlüs-

50 sel für den Algorithmus zur Entschlüsselung zu erhalten.

Fig. 5 stellt zusammenfassend einige wichtige Merkmale der vorliegenden Erfindung in der ersten Spalte sowie die dafür notwendigen Einträge in den variablen Teil 30 des Bestimmungsdatenblocks dar. Eine Ent-

55 schlüsselungsvorrichtung gemäß der vorliegenden Er- findung sollte selbstverständlich auch in der Lage sein, einen unverschlüsselten Bitstrom zu lesen, wobei dann auf die in Fig. 5 aufgeführten Einträge insgesamt verzichtet werden kann. Soll ein verschlüsselter Bitstrom

60 mit einem Demospieler, der die beschriebene Freischaltungsfunction implementiert, verwendet werden, so muß der Bestimmungsdatenblock der verschlüsselten Multimediataten zumindest den Freiindex 42 aufwei- sen.

65 Wie bereits erwähnt wurde, ist der Mengenindex 32 lediglich für eine effiziente Implementierung des erfin- dungsgemäßen Verfahrens erforderlich. Möchte ein Großhändler alle seine Benutzer mit seinen Produkten

gleichermaßen bedienen, so muß der Bestimmungsdatenblock der Multimediadaten der Großhändlerindex 36 besetzt sein. Optional kann auch der Freiindex 42 vorhanden sein, um lediglich bestimmten Benutzern das Abspielen von bestimmten Liedern zu erlauben.

Sollen alle Benutzer in den Genuß von Werken eines speziellen Lieferanten (d. h. des Besitzers des Urheberrechte) kommen können, können der Lieferantenindex und der Großhändlerindex besetzt sein. Optional kann auch ein Auslaufdatum 48 eingetragen sein.

Soll nur ein Benutzer auf ein spezielles Musikstück zugreifen können, so muß zusätzlich zum Lieferantenindex 34 und zum Großhändlerindex 36 der Benutzerindex 38 in den Bestimmungsdatenblock (10, 30) eingetragen sein.

Soll schließlich das beschriebene Herausforderungs-Antwort-Verfahren zum Einsatz kommen, was einen schnellen Zugriff auf eine große Datenbank von MMP-Multimediateien ermöglicht, so müssen selbstverständlich die Einträge Herausforderungsindex 44 sowie Antwortindex 46 besetzt sein. Für Fachleute ist es offensichtlich, daß die Freischaltung durch den Freiindex 42 bei einem Demospieler und beispielsweise das Herausforderungs-Antwort-Verfahren beliebig kombiniert werden können.

Die erfundungsgemäße Verschlüsselung bzw. Entschlüsselung liefert also eine Möglichkeit, um Multimediadaten bereits unmittelbar nach ihrer Erzeugung vor unerlaubtem Zugriff zu schützen, wobei die gesamte Kette vom Erzeuger zum Konsumenten einschließlich der Lagerung abgedeckt ist. Die vorliegende Erfindung zeichnet sich insbesondere durch die möglichen Merkmale der Teilverschlüsselung, der Erweiterbarkeit, d. h. der variable Teil des Bestimmungsdatenblocks kann beliebige weitere Funktionen aufnehmen, der maximalen Sicherheit gegen Fälschungen (d. h. die Prüfsumme 20) und der Verschlüsselung bestimmter Einträge in dem Bestimmungsdatenblock auf. Damit sind sowohl ein Schutz gegen eine unerlaubte Verwendung von Multimediadaten als auch durch Verwendung des Herausforderungs-Antwort-Gedankens eine effiziente Implementierung der Erfindung erreicht.

#### Patentansprüche

1. Verfahren zum Verschlüsseln von Multimediadaten, um eine verschlüsselte Multimediatei zu erhalten, die einen Bestimmungsdatenblock (10, 30) und einen Multimediatenblock aufweist, mit folgenden Schritten:

Eintragen eines Bestimmungsdaten-Verschlüsselungsindex (18) in den Bestimmungsdatenblock (10, 30), welcher auf einen zum Verschlüsseln eines Abschnitts des Bestimmungsdatenblocks (10, 30) zu verwendenden Bestimmungsdaten-Verschlüsselungsalgorithmus hinweist;

Eintragen eines Multimediaten-Verschlüsselungsindex (34, 36, 38, 44, 46) in den Bestimmungsdatenblock (10, 30), welcher auf einen zum Verschlüsseln zumindest eines Teils des Multimediatenblocks zu verwendenden Multimediaten-Verschlüsselungsalgorithmus hinweist;

Eintragen eines Freiindex (42) in den Bestimmungsdatenblock (10, 30), wobei der Freiindex (42) eine bestimmte Entschlüsselungsvorrichtung identifiziert, mit der ein Entschlüsseln der verschlüsselten Multimediaten über eine vorbestimmte Zeitdauer hinaus möglich ist;

5

Auswählen des Bestimmungsdaten-Verschlüsselungsalgorithmus aus einer Mehrzahl von Verschlüsselungsalgorithmen aufgrund des Bestimmungsdaten-Verschlüsselungsindex (18);

10

Auswählen des Multimediaten-Verschlüsselungsalgorithmus aus einer Mehrzahl von Verschlüsselungsalgorithmen aufgrund des Multimediaten-Verschlüsselungsindex (34, 36, 38, 44, 46); Verschlüsseln des Abschnitts des Bestimmungsdatenblocks (10, 30) mit dem Bestimmungsdaten-Verschlüsselungsalgorithmus, wobei der Abschnitt des Bestimmungsdatenblocks (10, 30) den Bestimmungsdaten-Verschlüsselungsindex nicht aufweist; und

15

zumindest teilweises Verschlüsseln des Multimediatenblocks mit dem Multimediaten-Verschlüsselungsalgorithmus.

20

2. Verfahren gemäß Anspruch 1, bei dem der Bestimmungsdatenblock (10, 30) vor den Multimediatenblock in eine Datei geschrieben wird.

25

3. Verfahren gemäß Anspruch 1 oder 2, das ferner folgenden Schritt aufweist:

Eintragen eines Mengenindex (32) in den Bestimmungsdatenblock (10, 30), der einen Anteil der zu verschlüsselnden Multimediaten von der Gesamtheit der Multimediaten in dem Multimediatenblock anzeigt, wodurch lediglich der durch den Mengenindex (32) bezeichnete Anteil der Multimediaten mittels des Multimediaten-Verschlüsselungsalgorithmus verschlüsselt wird.

30

4. Verfahren gemäß einem beliebigen der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Eintragen eines Lieferantenindex (34) in den Bestimmungsdatenblock (10, 30), der den Lieferanten anzeigt, der die Urherberrechte für die Multimediaten besitzt.

35

5. Verfahren gemäß einem beliebigen der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Eintragen eines Großhändlerindex (36) in den Bestimmungsdatenblock (10, 30), der den Großhändler anzeigt, der die Multimediaten anbietet.

40

6. Verfahren gemäß einem beliebigen der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Eintragen eines Benutzerindex (38) in den Bestimmungsdatenblock (10, 30), der den Benutzer anzeigt, zu dem die Multimediaten geliefert werden sollen.

45

7. Verfahren gemäß Anspruch 6, das ferner folgenden Schritt aufweist:

Eintragen eines Herausforderungsindex (44) und eines Antwortindex (46) in den Bestimmungsdatenblock (10, 30), wobei der Herausforderungsindex (44) und der Benutzerindex (38) zum Benutzerselektiven Abrufen von Multimediaten verwendet werden und zusammen mit dem Antwortindex (46) zum Entschlüsseln mittels eines zu verwendenden Entschlüsselungsalgorithmus verwendet werden, wobei aus dem Antwortindex (46) in Verbindung mit dem Benutzerindex (38) und dem Herausforderungsindex (44) ein Schlüssel (k) für den Verschlüsselungsalgorithmus zum Entschlüsseln bestimmt wird.

50

8. Verfahren gemäß Anspruch 7, das ferner folgenden Schritt aufweist:

Eintragen eines Flagindex (40) in den Bestim-

mungsdatenblock (10, 30), der anzeigt, ob bei der Verschlüsselung der Großhändlerindex (36), der Großhändlerindex (36) und der Benutzerindex (38) oder der Herausforderungsindex (44) und der Antwortindex (46) verwendet werden sollen.

9. Verfahren gemäß einem beliebigen der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Eintragen eines Auslaufindex (48) in den Bestimmungsdatenblock (10, 30), der anzeigt, wann eine Lizenz eines Benutzers zum Abrufen der Multimediatdaten ausläuft.

10. Verfahren gemäß einem beliebigen der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Eintragen eines Multimediaindex (50) in den Bestimmungsdatenblock (10, 30), der einzelne Musikstücke nach internationalem Standard identifiziert.

11. Verfahren gemäß Anspruch 10, das ferner folgenden Schritt aufweist:

Eintragen eines Benutzercodeindex (52) in den Bestimmungsdatenblock (10, 30), der Musikstücke identifiziert, die keinen Multimediaindex (50) aufweisen.

12. Verfahren gemäß einem beliebigen der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Eintragen eines Dateiindex (12) in den Bestimmungsdatenblock (10, 30), der die durch das Verschlüsselungsverfahren erzeugte Multimediatei, die den Bestimmungsdatenblock (10, 30) und den Multimediatdatenblock aufweist, allgemein kennzeichnet.

13. Verfahren gemäß einem beliebigen der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Eintragen eines Lägenindex (14) in den Bestimmungsdatenblock (10, 30), der die Länge des Bestimmungsdatenblocks (10, 30) anzeigt.

14. Verfahren gemäß Anspruch 13, das ferner folgenden Schritt aufweist:

Eintragen eines Versatzindex in den Bestimmungsdatenblock (10, 30), der einen Versatz zu einem möglichen weiteren Bestimmungsdatenblock (10, 30) in der verschlüsselten Multimediatei angezeigt.

15. Verfahren gemäß einem beliebigen der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Eintragen einer Prüfsumme (20) des Bestimmungsdatenblocks (10, 30) in den Bestimmungsdatenblock (10, 30).

16. Verfahren gemäß Anspruch 15, das ferner folgenden Schritt aufweist:

Verschlüsseln der Prüfsumme (20), des Freiindex (42), des Herausforderungsindex (44) und des Antwortindex (46); und

Eintragen der verschlüsselten Indizes in den Bestimmungsdatenblock (10, 30).

17. Verfahren gemäß Anspruch 15 oder 16, bei dem der Dateiindex (12), der Lägenindex (14), der Versatzindex (16), der Verschlüsselungsindex (18) und die Prüfsumme (20) in einem festen Teil des Bestimmungsdatenblocks vorhanden sind, während sich der Mengenindex (32), der Lieferantenindex (34), der Großhändlerindex (36), der Benutzerindex (38), der Flagindex (40), der Freiindex (42), der Herausforderungsindex (44), der Antwortindex (46), der

Auslaufindex (48), der Multimediaindex (50) und der Benutzercodeindex (52) in einem variablen Teil (30) des Bestimmungsdatenblocks (10, 30) befinden.

18. Verfahren gemäß Anspruch 17, bei dem jedem Eintrag in den variablen Teil (30) ein Hüllenblock (54) vorausgeht, der einen demselben folgenden Eintrag und dessen Länge spezifiziert.

19. Verfahren zum Entschlüsseln von Multimediatdaten, die nach Anspruch 1 verschlüsselt sind, mit folgenden Schritten:

Lesen des Bestimmungsdatenblocks (10, 30); Auswählen eines Bestimmungsdaten-Entschlüsselungsalgorithmen aus einer Mehrzahl von Entschlüsselungsalgorithmen aufgrund des Bestimmungsdaten-Verschlüsselungsindex (18);

Auswählen eines Multimediatdaten-Entschlüsselungsalgorithmen aus einer Mehrzahl von Entschlüsselungsalgorithmen aufgrund des Multimediatdaten-Verschlüsselungsindex (18);

Entschlüsseln des verschlüsselten Abschnitts des Bestimmungsdatenblocks (10, 30) unter Verwendung des Bestimmungsdaten-Entschlüsselungsalgoritmus; und

Entschlüsseln des Multimediatdatenblocks unter Verwendung des ausgewählten Multimediatdaten-Entschlüsselungsalgoritmus, wobei der Schritt des Entschlüsselns des Multimediatdatenblocks nur dann über eine vorbestimmte Zeitdauer hinaus fortgesetzt wird, wenn die Vorrichtung zum Entschlüsseln eine für den Freiindex (42) geeignete Einstellung aufweist.

20. Verfahren nach Anspruch 19 zum Entschlüsseln von Multimediatdaten, die nach Anspruch 1, 2 und 3 verschlüsselt sind,

bei dem lediglich der Anteil der Multimediatdaten in dem Multimediatdatenblock entschlüsselt wird, der durch den Mengenindex (32) angezeigt ist.

21. Verfahren gemäß einem der Ansprüche 19 oder 20, zum Entschlüsseln von Multimediatdaten, die nach Anspruch 1 bis 4 verschlüsselt sind,

bei dem der Schritt des Entschlüsselns des Multimediatdatenblocks nur dann durchgeführt wird, wenn ein Benutzer Produkte eines durch den Lieferantenindex (36) gekennzeichneten Lieferanten verwenden darf.

22. Verfahren gemäß einem der Ansprüche 19 bis 21 zum Entschlüsseln von Multimediatdaten, die nach Anspruch 1 bis 5 verschlüsselt sind,

bei dem der Schritt des Entschlüsselns des Multimediatdatenblocks nur dann durchgeführt wird, wenn ein Benutzer bei dem durch den Großhändlerindex (36) bezeichneten Großhändler autorisiert ist, Produkte desselben zu verwenden.

23. Verfahren nach einem der Ansprüche 19 bis 22 zum Entschlüsseln von Multimediatdaten, die nach Anspruch 6 verschlüsselt sind,

bei dem der Schritt des Entschlüsselns des Multimediatdatenblocks nur dann durchgeführt wird, wenn der durch den Benutzerindex (38) gekennzeichnete Benutzer die Multimediatdaten entschlüsselt.

24. Verfahren gemäß Anspruch 19 bis 23 zum Entschlüsseln von Multimediatdaten, die nach Anspruch 7 verschlüsselt sind,

bei dem der Schritt des Entschlüsselns des Multimediatdatenblocks das Berechnen eines für den ausgewählten Entschlüsselungsalgoritmus nötigen Entschlüsselungsschlüssel aufweist, der sich aus einer Kombination des Benutzerindex (38), des Her-

ausforderungsindex (44) und der Antwortindex (46) ergibt.

25. Vorrichtung zum Verschlüsseln von Multimediaträgerdaten, um eine verschlüsselte Multimediaträgerdatei zu erhalten, die einen Bestimmungsdatenblock (10, 30) und einen Multimediaträgerdatenblock aufweist, mit folgenden Merkmalen:

einer Einrichtung zum Eintragen eines Bestimmungsdaten-Verschlüsselungsindex (18) in den Bestimmungsdatenblock (10, 30), wobei der Bestimmungsdaten-Verschlüsselungsindex (18) auf einen zum Verschlüsseln eines Abschnitts des Bestimmungsdatenblocks (10, 30) zu verwendenden Bestimmungsdaten-Verschlüsselungsalgorithmus hinweist;

einer Einrichtung zum Eintragen eines Multimediaträgerdaten-Verschlüsselungsindex (34, 36, 38, 44, 46) in den Bestimmungsdatenblock (10, 30), wobei der Multimediaträgerdaten-Verschlüsselungsindex (34, 36, 38, 44, 46) auf einen zum Verschlüsseln zumindest eines Anteils des Multimediaträgerdatenblocks zu verwendenden Multimediaträgerdaten-Verschlüsselungsalgorithmus hinweist;

einer Einrichtung zum Eintragen eines Freiindex (42) in den Bestimmungsdatenblock (10, 30), wobei der Freiindex (42) die Vorrichtung zum Entschlüsseln identifiziert, mit der ein Entschlüsseln der verschlüsselten Multimediaträgerdaten über eine vorbestimmte Zeitdauer hinaus möglich ist;

einer Einrichtung zum Auswählen des Bestimmungsdaten-Verschlüsselungsalgorithmus aus einer Mehrzahl von Verschlüsselungsalgorithmen aufgrund des Bestimmungsdaten-Verschlüsselungsindex (18);

einer Einrichtung zum Auswählen des Multimediaträgerdaten-Verschlüsselungsalgorithmus aus einer Mehrzahl von Verschlüsselungsalgorithmen aufgrund des Multimediaträgerdaten-Verschlüsselungsindex (34, 36, 38, 44, 46);

einer Einrichtung zum Verschlüsseln des Abschnitts des Bestimmungsdatenblocks (10, 30) mit dem Bestimmungsdaten-Verschlüsselungsalgorithmus, wobei der Abschnitt des Bestimmungsdatenblocks (10, 30) den Bestimmungsdaten-Verschlüsselungsindex nicht aufweist; und

einer Einrichtung zum zumindest teilweisen Verschlüsseln des Multimediaträgerdatenblocks mit dem Multimediaträgerdaten-Verschlüsselungsalgorithmus.

26. Vorrichtung zum Verschlüsseln nach Anspruch

25, die ferner folgende Merkmale aufweist:

eine Einrichtung zum Eintragen eines Benutzerindex (38), der den Benutzer anzeigt, der die Multimediaträgerdaten benutzen kann, eines Herausforderungsindex (44) und eines Antwortindex (46) in einen Bestimmungsdatenblock (10, 30); und

eine Einrichtung zum Berechnen des Antwortindex (46) aus dem Benutzerindex (38), dem Herausforderungsindex (44) und einem für eine Verschlüsselungsvorrichtung spezifischen Schlüssels.

27. Vorrichtung zum Entschlüsseln von Multimediaträgerdaten, die nach Anspruch 1 verschlüsselt sind, mit folgenden Merkmalen:

einer Einrichtung zum Lesen des Bestimmungsdatenblocks (10, 30);

einer Einrichtung zum Auswählen eines Bestimmungsdaten-Verschlüsselungsalgorithmus aus einer Mehrzahl von Verschlüsselungsalgorithmen aufgrund des Bestimmungsdaten-Verschlüsselungs-

ungsindex (18); einer Einrichtung zum Auswählen eines Multimediaträgerdaten-Verschlüsselungsalgorithmus aus einer Mehrzahl von Verschlüsselungsalgorithmen aufgrund des Multimediaträgerdaten-Verschlüsselungsindex (18);

einer Einrichtung zum Entschlüsseln des verschlüsselten Abschnitts des Bestimmungsdatenblocks (10, 30) unter Verwendung des Bestimmungsdaten-Verschlüsselungsalgorithmus; und einer Einrichtung zum Entschlüsseln des Multimediaträgerdatenblocks unter Verwendung des ausgewählten Multimediaträgerdaten-Verschlüsselungsalgorithmus, wobei die Vorrichtung zum Entschlüsseln der Multimediaträgerdaten nur dann über eine vorbestimmte Zeitdauer hinaus den Multimediaträgerdatenblock entschlüsselt, wenn die Vorrichtung eine für den Freiindex (42) geeignete Einstellung aufweist.

28. Vorrichtung zum Entschlüsseln nach Anspruch 27, die ferner eine Einrichtung zum Berechnen eines Schlüssels für den ausgewählten Multimediaträgerdaten-Verschlüsselungsalgorithmus aus einer Kombination eines in dem Bestimmungsdatenblock (10, 30) vorhandenen Benutzerindex (38), eines in demselben vorhandenen Herausforderungsindex (44) und eines in demselben vorhandenen Antwortindex (46) aufweist.

Hierzu 3 Seite(n) Zeichnungen

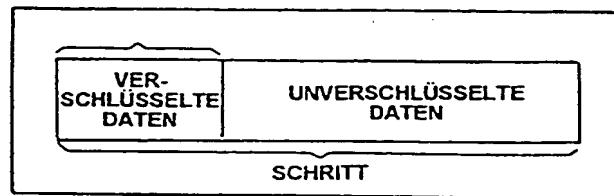
Nummer:

DE 196 25 635 C1

Int. Cl.<sup>6</sup>:

H 04 L 9/32

Veröffentlichungstag: 4. Dezember 1997

*FIG.3*

S 4 -

NAME DES EINTRAGS	GRÖSSE	NAME DES UNTEREINTRAGS		VER-Schlüssel.?
EINTRAG	4 BYTE	EINTRAGSIDENTIFIKATION EINTRAGSLÄNGE		NEIN

*FIG.4*

	MENGENINDEX 32	LIEFERANTENINDEX 34	GROSSHÄNDLER- INDEX 36	BENUTZERINDEX 38	FREIINDEX 42	HERAUFORDERUNGS- INDEX 44	ANTWORTINDEX 46	AUSLAUFDATUM 48
UNVERSCHÜSSELTERR BITSTROM								
VERSCHLÜSSELTERR BITSTROM MIT DEMOSPIELER ( FREISCHALTUNG )	X				X			
VERSCHLÜSSELTERR BITSTROM FÜR BENUTZER EINES SPEZIFISCHEN GROSSHANLDERS ( DEMOSPIELER FREISCHALTUNG )	X		X		X			
VERSCHLÜSSELTERR BITSTROM FÜR ALLE BENUTZER EINES SPEZIFISCHEN LIEFERANTEN	X	X	X				(X)	
VERSCHLÜSSELTERR BITSTROM FÜR EINEN BENUTZER EINES SPEZIFISCHEN LIEFERANTEN	X	X	X	X			(X)	
VERSCHLÜSSELTERR BITSTROM FÜR EINEN BENUTZER EINES SPEZIFISCHEN LIEFERANTEN ( SCHNELLERER DATENBANKZUGRIFF )	X	X	X	X		X	X	(X)

*FIG.5*

	NAME DES EINTRAGS	GRÖSSE	NAME DES UNTER-EINTRAGS	GRÖSSE	VER-Schlüss.?
12	DATENINDEX	4 BYTE	IDENTIFIZIERER VERSION	24 BYTE 8 BYTE	NEIN
14	LÄNGENINDEX	4 BYTE	BESTIMMD.-BLOCKLÄNGE	32 BYTE	NEIN
16	VERSATZINDEX	4 BYTE	VERSATZ	32 BYTE	
18	VERSCHLÜSSE-LUNGSDINDEX	4 BYTE	VERFAHREN SCHLÜSSEL	16 BYTE 16 BYTE	NEIN
VARIABLER TEIL DES BESTIMMUNGSDATENBLOCKS ( SIEHE FIG.2 )					
20	PRÜFSUMME	16 BYTE	MDS-FINGERABDRUCK	128 BYTE	JA

FIG.1

	ID	NAME DES EINTR.	GRÖSSE	NAME DES UNTER-EINTRAGS	GRÖSSE	VER-Schlüss.?
32	0 x 01	MENGENINDEX	8 BYTE	SCHRITT MENGE	16 BIT 16 BIT	NEIN
34	0 x 02	LIEFERANTENINDEX	8 BYTE	LIEFERANT	32 BIT	NEIN
36	0 x 03	GROSSHÄNDLERIND.	8 BYTE	GROSSHÄNDLER	32 BIT	NEIN
38	0 x 04	BENUTZERINDEX	8 BYTE	BENUTZER	32 BIT	NEIN
40	0 x 05	FLAGINDEX	8 BYTE	GEHEIM REGISTRIERUNG HERAUSFORDERUNG	1 BIT 1 BIT 1 BIT	NEIN
42	0 x 06	FREIINDEX	20 BYTE	SERIENNUMMER BENUTZERDATEN	32 BIT 96 BIT	JA
44	0 x 07	HERAUSFORDE-RUNGSINDEX	20 BYTE	DECODIERERTYP CODIEREVERSION DECOD.-ZUSTAND GROSSHÄNDLERINDEX BENUTZERINDEX BENUTZERDATEN	4 BIT 4 BIT 8 BIT 32 BIT 32 BIT 46 BIT	JA
46	0 x 08	ANTWORTINDEX	20 BYTE	ANTWORTINDEX	128 BIT	
48	0 x 09	AUSLAUFINDEX	8 BYTE	AUSLAUFDATUM	32 BIT	NEIN
50	0 x 0a	MULTIMEDIA-INDEX	16 BYTE	LANDCODE EIGENTÜMERCODE JAHR BEZEICHNUNGSCODE	16 BIT 24 BIT 16 BIT 40 BIT	
52	0 x 0b	BENUTZERCODE-INDEX	16 BYTE	BENUTZERCODE	32 BIT	NEIN

FIG.2